

Solutions by radicals at singular values k_N from new class invariants for $N \equiv 3 \pmod{8}$

David Broadhurst*

July 31, 2008

Abstract

For square-free $N \equiv 3 \pmod{8}$ and N coprime to 3, I show how to reduce the singular value k_N to radicals, using a novel pair $[f, g]$ of real numbers that are algebraic integers of the Hilbert class field of $Q(\sqrt{-N})$. One is a class invariant of modular level 48, with a growth $g = \alpha(N) \exp(\pi\sqrt{N}/48) + o(1)$, where $\alpha(N) \in [-\sqrt{2}, \sqrt{2}]$ is uniquely determined by the residue of N modulo 64. Hence g is a very economical generator of the class field. For prime $N \equiv 3 \pmod{4}$, I conjecture that the Chowla–Selberg formula provides an algebraic *unit* of the class field and determine its minimal polynomial for the 155 cases with $N < 2000$. For $N = 2317723$, with class number $h(-N) = 105$, I compute the minimal polynomial of g in 90 milliseconds. Its height is smaller than the *cube* root of the height of the generating polynomial found by the double eta-quotient method of *Pari-GP*. I reduce the complete elliptic integral $K_{2317723}$ to radicals and values of the Γ function, by determining the Chowla–Selberg unit and solving the septic, quintic and cubic equations that generate sub-fields of the class field. I conclude that the residue 3 modulo 8, initially discarded in elliptic curve primality proving, outperforms the residue 7.

1 Introduction

The N th singular value [29, 4] is the algebraic number $k_N \in [0, 1]$ for which

$$\text{AGM}\left(1, \sqrt{1 - k_N^2}\right) = \sqrt{N} \text{AGM}(1, k_N) \quad (1)$$

where the arithmetic-geometric mean (AGM) is obtained by iterating the rapidly convergent process [7] $\text{AGM}(a, b) = \text{AGM}\left((a+b)/2, \sqrt{ab}\right)$. For square-free $N \equiv 3 \pmod{8}$, with N coprime to 3,

$$k_N^2 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{16}{r^{24}}} \quad (2)$$

*Department of Physics and Astronomy, The Open University, Milton Keynes, MK7 6AA, United Kingdom, D.Broadhurst@open.ac.uk.

is determined by an algebraic number $r > 2^{\frac{1}{4}}$ that is given by a Weber function [30, 1, 33, 16, 21, 26] and has a minimal polynomial of degree $3h$, where $h = h(-N)$ is the class number of the imaginary quadratic field $Q(\sqrt{-N})$.

For square-free $N \equiv 3 \pmod{4}$, the complete elliptic integral

$$K_N = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k_N^2x^2)}} = \frac{\pi}{2} \frac{1}{\text{AGM}\left(1, \sqrt{1-k_N^2}\right)} \quad (3)$$

is reducible to the Γ values [13, 27, 34] in

$$G_N = \prod_{k=1}^N \left[\Gamma\left(\frac{k}{N}\right) \right]^{\left(\frac{-N}{k}\right)} \quad (4)$$

with exponents given by the Legendre–Jacobi–Kronecker symbol $\left(\frac{-N}{k}\right)$. For $N > 3$, this reduction takes the form

$$K_N = \left(\frac{r}{2}\right)^2 \sqrt{\frac{2\pi}{N} (\lambda^4 G_N)^{\frac{1}{h}}} \quad (5)$$

where $\lambda > 0$ is an algebraic number. As noted in [13, Eq. 8], $\lambda = 1$ when $h(-N) = 1$. Moreover, I conjecture in this paper that λ is an algebraic *unit* of the Hilbert class field when $h(-N)$ is odd, i.e. for prime $N > 3$ congruent to 3 modulo 4.

I shall describe how r and λ were reduced to radicals in the case $N = 2317723$, with class number $h(-N) = 105$. To achieve this reduction, I construct, in Section 4.2, a pair of class invariants, one of which appears to outperform the `quadhilbert` procedure of *Pari-GP*, in regard of the economy with which it generates the class field.

2 Chowla–Selberg formula

It is not necessary to compute N values of the Γ function to evaluate G_N at high precision. Instead we may use h values of the Dedekind eta function

$$\eta(z) = \exp(\pi iz/12) \prod_{k=1}^{\infty} (1 - \exp(2\pi i k z)) = \sum_{n=-\infty}^{\infty} (-1)^n \exp((6n+1)^2 \pi iz/12) \quad (6)$$

to evaluate G_N using the Chowla–Selberg formula [27, Eq. 2, p. 110]

$$\prod_{k=1}^N \left[\Gamma\left(\frac{k}{N}\right) \right]^{\left(\frac{-N}{k}\right)} = (2\pi N)^h \prod_{[a,b,c] \in H} \frac{1}{a} \left| \eta\left(\frac{b + \sqrt{-N}}{2a}\right) \right|^4 \quad (7)$$

for square-free $N \equiv 3 \pmod{4}$ and $N > 3$. For other cases, including non-fundamental discriminants, see [17]. In (7), the product runs over the strict equivalence classes $[a, b, c]$ of primitive integral binary quadratic forms $ax^2 + bxy + cy^2$ with discriminant $b^2 - 4ac = -N$. These equivalence classes form an Abelian group H , by Gauss’s composition of quadratic forms, and the order of H is the class number $h = h(-N)$. It is remarked in [18] that publication of this striking formula was delayed for 18 years, between its discovery at the time of the Chowla–Selberg paper [13] of 1949 and its appearance in the Selberg–Chowla paper [27] of 1967. For precursors of this formula, see [23].

2.1 A conjecture for prime discriminants

For square-free positive $N \equiv 3 \pmod{4}$, I define

$$\lambda = \prod_{[a,b,c] \in H} a^{\frac{1}{4}} \left| \frac{\eta\left(\frac{1+\sqrt{-N}}{2}\right)}{\eta\left(\frac{b+\sqrt{-N}}{2a}\right)} \right| \quad (8)$$

where the product runs over the equivalence classes for discriminant $b^2 - 4ac = -N$.

Conjecture 1: For prime $N \equiv 3 \pmod{4}$, λ is a unit of the Hilbert class field of $Q(\sqrt{-N})$.

Remarks:

1. I have verified this in the 155 cases with $N < 2000$.
2. For each of these cases, the minimal polynomial $L(x)$ of λ is available¹ in a file `lambdaCS.txt` which is read by `lambdaCS.gp` with output in `lambdaCS.out` that confirms, at a precision of 15,000 digits, that $L(\lambda) = 0$ and that L generates the same field as the `quadhilbert` procedure of *Pari-GP*.
3. In each of these cases, $L(x)$ is a monic polynomial with $L(0) = -1$ and hence λ is a unit of the class field.
4. For $N = 2317723$, the Hilbert class group is cyclic and is generated by the equivalence class $[a, b, c] = [151, -91, 3851]$, with order $h(-N) = 105$. In Section 5, I describe how 15,000 digits of λ were used to reduce it to a unit, which was then checked at 40,000 digits of precision.
5. John Zucker and I have investigated some composite discriminants, finding that λ^2 is a unit when N is a product of distinct primes greater than 3. I have verified this for squarefree $N < 2000$ with $N \equiv 3 \pmod{4}$ and coprime to 3. I have not yet found a simple criterion that determines why $N = 7 \times 11 \times 13 \times 19 = 19019$ yields λ as a unit, while for $N = 7 \times 11 \times 23 = 1771$ one must take λ^2 to form a unit.

3 Hilbert class field

The Hilbert class field of $Q(\sqrt{-N})$ is generated by the polynomial [14, Th. 7.2.14]

$$P(x) = \prod_{[a,b,c] \in H} \left(x - j\left(\frac{b+\sqrt{-N}}{2a}\right) \right) \quad (9)$$

where

$$j(z) = \left(\left(\frac{\eta(z/2)}{\eta(z)} \right)^{16} + 16 \left(\frac{\eta(z)}{\eta(z/2)} \right)^8 \right)^3. \quad (10)$$

As shown in [30, Sect. 125, p. 461], a real root of $P(x)$ is supplied by

$$\left(\frac{256}{r^{16}} - r^8 \right)^3 = j\left(\frac{1+\sqrt{-N}}{2}\right). \quad (11)$$

For $N = 2317723$, $P(x)$ is a polynomial of degree 105, whose integer coefficients have up to 3050 decimal digits, making it rather difficult to reduce its roots to a set of simple

¹From the directory <http://paftp.open.ac.uk/pub/staff/ftp/dbroadhu/K2317723/>.

radicals. Fortunately, we do not need to use $P(x)$. A more convenient polynomial that generates the same number field will serve our purpose. Using a class invariant defined in Section 4.2, I found that the Hilbert class field of $Q(\sqrt{-2317723})$ is generated by a compositum of three polynomials that generate its sub-fields of prime degree, namely

$$Q_7(x) = x^7 - 323x^5 - 6057x^4 - 35434x^3 - 186299x^2 - 1450032x - 19143360 \quad (12)$$

$$Q_5(y) = y^5 - y^4 - 339y^3 - 7879y^2 + 146334y - 566316 \quad (13)$$

$$Q_3(z) = z^3 - z^2 - 59z - 322 \quad (14)$$

where Q_p has discriminant

$$D_p = f_p^2(-N)^{\frac{p-1}{2}} \quad (15)$$

with an index f_p . The indices

$$f_3 = 1, \quad f_5 = 2^4 \times 3 \times 5^2 \times 11 \times 17 \times 47, \quad f_7 = 2^{10} \times 3^2 \times 19^2 \times 61 \times f_5 \quad (16)$$

fortunately contain no prime greater than 61.

4 An efficient pair of class invariants

The algebraic number r in (2) is the real root of a monic cubic polynomial with coefficients in the Hilbert class field. These coefficients are algebraically constrained by the condition that [30]

$$\gamma_2 = \frac{256}{r^{16}} - r^8 \quad (17)$$

generates the Hilbert class field, while the minimal polynomial for r has degree $3h$ and generates a cubic relative extension.

For each of the 198 primes congruent to 3 modulo 8 and less than 6000, I found that the cubic relative extension takes the form [9]

$$r^3 - 2(fr^2 + gr + 1) = 0 \quad (18)$$

where f and g are algebraic integers of the Hilbert class field. I then found that these algebraic integers obey the constraint

$$2f^4 - 16f^3g^2 + 20f^2g^4 - 12f^2g - 8fg^6 + 16fg^3 - 2f + g^8 - 4g^5 + 3g^2 = 0 \quad (19)$$

which indeed ensures that r does not appear in

$$-\frac{\gamma_2}{32} = 8f^8 + 32f^6g + 16f^5 + 40f^4g^2 + 32f^3g + 16f^2g^3 + 6f^2 + 12fg^2 + g^4 + 2g \quad (20)$$

as may be confirmed by using (18) to eliminate powers r^j with $j \geq 3$ from (17) and then using (19) to eliminate powers g^k with $k \geq 8$.

A particularly simple example [30, Table VI, p. 725] is provided by $N = 163$, the largest number for which $h(-N) = 1$, where the integer pair $[f, g] = [3, -2]$ determines the well-known 18-digit integer [14, Sect. 7.2.3]

$$-j \left(\frac{1 + \sqrt{-163}}{2} \right) = 262537412640768000 \quad (21)$$

that differs from $\exp(\pi\sqrt{163})$ by less than 3 parts in 10^{30} and is here obtained by evaluating $-\gamma_2^3$, using (20). Hence $[f, g] = [3, -2]$ is a Diophantine solution of (19).

4.1 A signature for $N \equiv 3 \pmod{8}$

I began my investigations by considering prime values of $N \equiv 3 \pmod{8}$, since those yield a Chowla–Selberg unit, according to Conjecture 1. Studying such primes, I discovered a signature, comprising a triplet of signs $[S_1, S_2, S_3]$ that eventually enabled me to construct a pair of class invariants for any number congruent to 3 modulo 8 and coprime to 3.

I arrived at this signature by using (18) to eliminate f from (19), obtaining an octic equation for g . After some manipulations, I was able to solve this by taking 3 square roots. The general solution for the octic has the form

$$g = -\frac{1}{r} + S_1 \left(r + S_2 \left(\frac{r^2}{2} + S_3 \left(\frac{r^4}{8} - \frac{1}{r^8} \right)^{\frac{1}{2}} \right)^{\frac{1}{2}} \right)^{\frac{1}{2}} \quad (22)$$

with signs $S_j = \pm 1$.

By conjecture, precisely one of the 8 choices of signs gives an algebraic integer of the Hilbert class field of $Q(\sqrt{-N})$. If we know this signature, the problem of identifying k_N as an algebraic number becomes *much* more tractable than previously supposed, since instead of having to find an integer relation between $3h + 1$ numbers, namely r and an integral basis for a cubic relative extension of the Hilbert class field, we now need a pair of relations between merely $h + 2$ numbers, namely $[f, g]$ and an integral basis for the Hilbert class field itself. At large N , the coefficients in the minimal polynomial of $g = O(\sqrt{r})$ have, typically, 48 times fewer digits than those in the Hilbert polynomial (9).

I determined the signatures of the 198 primes $N \equiv 3 \pmod{8}$ with $N < 6000$ by trial and error, using the `lindep` procedure of *Pari-GP* to search for a integer relation between the unique real embedding of the integral basis `nfinit(quadhilbert(-N)).zk` and numerical evaluations of (22) in each of 8 possible cases. For each prime, I found precisely one valid signature. Then I listed the first 12 primes for each signature, obtaining the sequences

$[-1, -1, -1]$: 163, 227, 419, 547, 739, 1123, 1187, 1571, 1699, 2083, 2339, 2467
$[-1, -1, +1]$: 11, 139, 331, 523, 587, 907, 971, 1163, 1291, 1483, 1867, 1931
$[-1, +1, -1]$: 179, 307, 499, 563, 691, 883, 947, 1459, 1523, 1907, 2099, 2803
$[-1, +1, +1]$: 59, 251, 379, 443, 571, 827, 1019, 1531, 1723, 1787, 1979, 2683
$[+1, -1, -1]$: 3, 67, 131, 643, 1091, 1283, 1667, 1987, 2179, 2243, 2371, 2819
$[+1, -1, +1]$: 43, 107, 491, 619, 683, 811, 1259, 1451, 1579, 2027, 2347, 2411
$[+1, +1, -1]$: 19, 83, 211, 467, 659, 787, 1171, 1427, 1619, 1747, 1811, 2003
$[+1, +1, +1]$: 283, 347, 859, 1051, 1307, 1499, 1627, 2011, 2203, 2267, 2459, 2843

which led me to conjecture, as these 8 lists were slowly growing, that the signature of a prime congruent to 3 modulo 8 is uniquely determined by its residue modulo 64, as indeed turned out to be the case for the rest of the sample of 198 primes.

I then checked that this is also the case for all the composite integers less than 3500 that are congruent to 3 modulo 8 and coprime to 3, using the `nfisom` routine of *Pari-GP* in situations for which `quadhilbert` did not furnish a polynomial with a real root. (I thank Karim Belabas for this workaround.)

Thus, for each square-free positive integer N that is congruent to 3 modulo 8 and is coprime to 3 (and also for $N = 3$ itself) there appears to be a unique signature $[S_1, S_2, S_3]$, determined by the residue of N modulo 64, such that (22) yields an algebraic integer of the class field.

4.2 Construction and conjecture modulo 64

For positive integer N congruent to 3 modulo 8, I define a signature

$$[S_1, S_2, S_3] = \begin{cases} [-1, -1, -1] & \text{for } N \equiv 35 \pmod{64} \\ [-1, -1, +1] & \text{for } N \equiv 11 \pmod{64} \\ [-1, +1, -1] & \text{for } N \equiv 51 \pmod{64} \\ [-1, +1, +1] & \text{for } N \equiv 59 \pmod{64} \\ [+1, -1, -1] & \text{for } N \equiv 3 \pmod{64} \\ [+1, -1, +1] & \text{for } N \equiv 43 \pmod{64} \\ [+1, +1, -1] & \text{for } N \equiv 19 \pmod{64} \\ [+1, +1, +1] & \text{for } N \equiv 27 \pmod{64} \end{cases} \quad (23)$$

and a pair of algebraic numbers

$$[f, g] = \left[\frac{r}{2} - \frac{s}{\sqrt{r}}, -\frac{1}{r} + s\sqrt{r} \right] \quad (24)$$

where

$$r = \exp(-\pi i/24) \frac{\eta\left(\frac{1+\sqrt{-N}}{2}\right)}{\eta(\sqrt{-N})} \quad (25)$$

$$s = S_1 \left(1 + S_2 \left(\frac{1}{2} + S_3 \left(\frac{1}{8} - \frac{1}{r^{12}} \right)^{\frac{1}{2}} \right)^{\frac{1}{2}} \right)^{\frac{1}{2}}. \quad (26)$$

Conjecture 2: For every square-free positive integer N congruent to 3 modulo 8 and coprime to 3, the Hilbert class field of $Q(\sqrt{-N})$ is generated by at least one of $[f, g]$ and for $N > 1099$ it is generated by both.

Remarks:

1. I have checked that the minimal polynomials of $f = f(N)$ and $g = g(N)$ have degree $h = h(-N)$ for all of the cases in Conjecture 2 with $1099 < N < 100000$.
2. There are 7 cases with $N \leq 1099$ in which only one of $[f, g]$ generates the Hilbert class field, while the other generates a sub-field.
3. Five of these yield the integers $f(83) = 1$, $f(91) = 1$, $g(331) = -1$, $g(427) = 1$, $g(907) = -2$ and were noted in [24], with three cases appearing in [33, Table 5].
4. For $N = 715$, with $h = 4$, the minimal polynomial of g is $x^2 + x - 1$.
5. For $N = 1099$, with $h = 6$, it is $x^3 + x^2 - x + 6$.
6. In the cases $N = 11, 19, 43, 67, 163$, with $h = 1$, the $[f, g]$ pairs are $[1, -1]$, $[0, 1]$, $[1, 0]$, $[1, 1]$, $[3, -2]$, all of which were noted in [30, Table VI].
7. Apart from the 10 cases noted above, no other value of $N < 1000000$ produces an integer. (The integers $f(3) = g(3) = f(27) = 0$ do not fall within Conjecture 2.)
8. For $N < 3500$, I have verified that whenever the minimal polynomial of f or g has degree h the field which it generates is isomorphic to that generated by the `quadhilbert` procedure of *Pari-GP*.
9. I have performed the same tests for prime $N < 6000$.
10. At large N , the minimal polynomial of g provides a rather economical generator of the field. For $N = 2317723$, it may be computed in less than 100 milliseconds and has a height less than the *cube* root of the height of the `quadhilbert` polynomial.

4.3 Minimal polynomials

The algebraic numbers f and g are, by construction, roots of the polynomials

$$F(x) = \prod_{j=1}^h \left(x - \frac{r_{j,1}}{2} - \frac{r_{j,2}}{2} - \frac{r_{j,3}}{2} \right) \quad (27)$$

$$G(x) = \prod_{j=1}^h \left(x + \frac{1}{r_{j,1}} + \frac{1}{r_{j,2}} + \frac{1}{r_{j,3}} \right) \quad (28)$$

where $r_{j,k}$ is a labelling of the roots of the minimal polynomial of r such that

$$\gamma_2(r_{j,1}) = \gamma_2(r_{j,2}) = \gamma_2(r_{j,3}) \quad (29)$$

with $\gamma_2(r) = 256/r^{16} - r^8$. Conjecture 2 asserts, *inter alia*, that at least one of these polynomials is irreducible and generates the Hilbert class field.

To compute the polynomials, we may use Reinier Bröker's fine formula [11, Th. 6.3, p. 106] for the root associated to the equivalence class $[a, b, c]$ of binary quadratic forms with discriminant $b^2 - 4ac = -4N$. Denoting $z = (b/2 + \sqrt{-N})/a$, this root is

$$R(a, b, c) = \begin{cases} -(-1)^{\frac{a^2-1}{8}} \exp\left(-\frac{b(ac^2-a-2c)}{48} \pi i\right) \frac{\eta(z/2)}{\eta(z)} & \text{if } c \text{ is even} \\ -(-1)^{\frac{c^2-1}{8}} \exp\left(-\frac{b(c-a-5ac^2)}{48} \pi i\right) \sqrt{2} \frac{\eta(2z)}{\eta(z)} & \text{if } a \text{ is even} \\ \exp\left(-\frac{b(c-a-a^2c)+2}{48} \pi i\right) \frac{\eta((1+z)/2)}{\eta(z)} & \text{otherwise} \end{cases} \quad (30)$$

where I have written the Weber functions as explicit eta quotients. I remark that $R(1, 0, N) = r$ determines the N th singular value (2) and that at least one of $[a, c]$ is odd, since b is even.

When the class group for discriminant $-4N$ is generated cyclicly, by a single class with order $3h$, there is a very simple procedure to generate the roots with a labelling that respects the condition (29): we may compute $r_{j,k}$ by applying (30) to the reduced form obtained by raising the generator to the power $j + (k-1)h$. If there are sub-groups, a little book-keeping is required to ensure that the roots are slotted into (27,28) in a manner that respects condition (29). I ordered the roots by size of the real parts of their γ_2 values and then inspected the signs of the imaginary part of γ_2

For $N > 1099$, the minimal polynomial G is a rather economical generator of the Hilbert class field. In the rather simple example of $N = 1571$, with $h = 17$, I obtained

$$\begin{aligned} G(x) = & x^{17} + 14x^{16} + 38x^{15} + 19x^{14} + 83x^{13} + 440x^{12} + 275x^{11} - 507x^{10} + 384x^9 \\ & + 541x^8 - 1343x^7 - 88x^6 + 712x^5 + 585x^4 - 1254x^3 + 852x^2 - 304x + 64 \end{aligned} \quad (31)$$

whose index

$$2^{37} \times 13^2 \times 17^2 \times 41 \times 43 \times 139 \times 2083 \times 34259 = 117388472496907896691997278208 \quad (32)$$

has merely 30 digits. By contrast the polynomial obtained in [11, p. 152], using a double eta-quotient [25, 26, 15] of the form

$$w_{p,q}(z) = \frac{\eta\left(\frac{z}{p}\right)\eta\left(\frac{z}{q}\right)}{\eta(z)\eta\left(\frac{z}{pq}\right)}, \quad (33)$$

with $[p, q] = [5, 7]$, has a 52-digit index, while `quadhilbert` yields a 60-digit index, using $[p, q] = [29, 31]$.

The economy of G is also reflected in the storage for the integral basis obtained by outputting `nfini(G).zk` from *Pari-GP*, which produces a file of less than 12 kilobytes, while `nfini(quadhilbert(-1571)).zk` produces more than 29 kilobytes. This is because large divisors of the index occur in the denominators of the rational elements of the matrix that transforms powers of the root to an integral basis.

5 Reduction to simple radicals for $N = 2317723$

For $N = 2317723$, I used the generator $[a, b, c] = [604, 422, 3911]$, with order 315, to obtain the polynomials $[F, G]$ from (27,28) in 90 milliseconds. Their indices in the class field have 10,756 and 5,815 digits, respectively. By way of comparison, the `quadhilbert` routine of *Pari-GP* gave an index with 20,075 digits. The height of G has 65 digits, while a 204-digit height was produced by `quadhilbert`. Using G , I found the sub-fields (12,13,14).

5.1 The elliptic integral $K_{2317723}$

Inspired by the results in [3, pp. 238–247], obtained by Jon Borwein and John Zucker for elliptic integrals K_N with $N \leq 100$, my goal was to reduce the elliptic integral $K_{2317723}$ to Γ values and the simplest possible radicals, which I took to be those generated by the polynomials Q_7 , Q_5 and Q_3 in (12,13,14), whose indices in sub-fields of the Hilbert class field contain no prime greater than 61. By contrast, a compositum of these polynomials gave a 7419-digit index.

Nonetheless, I found it convenient to construct, for intermediate purposes, a local integral basis from this compositum and then to use `lindep` to obtain the coefficients of $[f, g, \lambda]$ in this basis. The reason is simple: this is a triplet of algebraic integers, so by using an integral basis we ensure that no large denominator may leak into the Q -linear relations and thereby inflate the typical size of numerators in rational coefficients.

Hence the results were, in the first instance, in terms of a rather unwieldy (yet computationally effective) integral basis, occupying 74 Megabytes of disk space. However, it was possible to shrink this data set, very dramatically.

5.2 Reduction to monomials

Next, I transformed $[f, g, \lambda]$ from the integral basis to the 105 monomials $x^i y^j z^k$, with $i < 7$, $j < 5$ and $k < 3$, where x , y and z are the unique real roots of $Q_7(x) = 0$, $Q_5(y) = 0$ and $Q_3(z) = 0$. Then *Pari-GP* found that the `content` of g is $1/C$, where

$$C = 2^8 \times 3^2 \times 5^3 \times 11^2 \times 17^2 \times 19^2 \times 47^2 \times 61 \times 2317723 = 1135455149209896386784000 \quad (34)$$

has 25 digits. The resulting compact integer data for the vector $V = [f, g, \lambda]$ is available (see the first footnote) in the form of a 32-kilobyte file `K2317723.txt` that achieves a 2300-fold compression of the data from the integral basis.

I remark that my intermediate use of an integral basis had the merit of reducing the working precision required for the reduction of λ to radicals by roughly 2,500 decimal digits, i.e. by about 25 digits per term in the reduction of the unit λ to an integral basis of the class field.

It seemed to me to be beyond reasonable expectation that *Pari-GP* might determine a system of fundamental units for the class field of $Q(\sqrt{-N})$ with $N = 2317723$. Hence I used only `nfin` at $N = 2317723$, while the more time-consuming procedure `bnfin` was used to good effect for $N < 6000$.

5.3 Solution of sub-fields by radicals

To complete the reduction to simple radicals, I needed to determine the real roots of the equations $Q_7(x) = 0$, $Q_5(y) = 0$, $Q_3(z) = 0$ and then, from f and g , the real root r of the cubic (18). It is elementary to solve a cubic by radicals. In particular,

$$z = \frac{1}{3} + \left(\frac{9227}{54} + \sqrt{\frac{2317723}{108}} \right)^{\frac{1}{3}} + \left(\frac{9227}{54} - \sqrt{\frac{2317723}{108}} \right)^{\frac{1}{3}} \quad (35)$$

is the unique real root of $Q_3(z) = 0$. To solve the quintic, we may compute the real parts

$$\begin{aligned} u_n = \Re \Big[& -(650272782 - 564880\sqrt{-2317723}) \exp(2\pi i n/5) \\ & -(1703074422 - 359490\sqrt{-2317723}) \exp(4\pi i n/5) \Big] \end{aligned} \quad (36)$$

for $n = 1 \dots 4$, using $4 \cos(\pi/5) = 1 + \sqrt{5}$. Then

$$y = \frac{1 + u_1^{\frac{1}{5}} + u_2^{\frac{1}{5}} - (-u_3)^{\frac{1}{5}} + u_4^{\frac{1}{5}}}{5} \quad (37)$$

is the unique real root of $Q_5(y) = 0$. To solve the septic, we may compute the real parts

$$\begin{aligned} v_n = \Re \Big[& -(1959346982341 + 140861987\sqrt{-2317723}) \exp(2\pi i n/7) \\ & -(686210881202 - 650234914\sqrt{-2317723}) \exp(4\pi i n/7) \\ & -(1670361863821 + 547274245\sqrt{-2317723}) \exp(6\pi i n/7) \Big] \end{aligned} \quad (38)$$

for $n = 1 \dots 6$, using

$$6 \cos(\pi/7) = 1 + \left(\frac{-7 + 7\sqrt{-27}}{2} \right)^{\frac{1}{3}} + \left(\frac{-7 - 7\sqrt{-27}}{2} \right)^{\frac{1}{3}} \quad (39)$$

and then

$$x = \frac{v_1^{\frac{1}{7}} - (-v_2)^{\frac{1}{7}} + v_3^{\frac{1}{7}} + v_4^{\frac{1}{7}} + v_5^{\frac{1}{7}} + v_6^{\frac{1}{7}}}{7} \quad (40)$$

is the unique real root of $Q_7(x) = 0$.

The algebraic integers in u_n and v_n were found at 38-digit precision, using the method outlined in [20, Chap. 3.1] and there exemplified by the quintic that generates the Hilbert class field of $Q(\sqrt{-47})$. As remarked in [6, VI-5] that quintic was solved by G.P. Young [32] in 1888. For G.N. Watson's comments on Young, see [5]. For J.M. Whittaker's comments on Watson, see [31]. For the inspirational role of Srinivasa Ramanujan, see [4].

5.4 Numerical checks

At no stage in the reduction of $[f, g, \lambda]$ to such simple radicals was it necessary to use a working precision above 15,000 digits. The results were then checked at a precision of 40,000 digits. For the singular value, that is very easy, since we need only take seventh, fifth, cube and square roots and check the relation between a pair AGMs in (1). To check the elliptic integral, I evaluated the Chowla–Selberg formula (7) at a precision of 40,000 digits. As a final check that no stray factor had been overlooked in going from the Γ values in (4) to the η values in (7), I evaluated 2,317,723 values of the Γ function, at 38-digit precision, and combined them with the Kronecker symbol, obtaining agreement with (5). The checking programme `K2317723.gp` and its output `K2317723.out` are in the same directory as the monomial coefficients, with a URL given in the first footnote.

6 Comments and conclusion

As announced in [9, 10], I had earlier reduced the elliptic integrals K_{34483} and $K_{1242763}$ to algebraic numbers and Γ values, following the identification of elliptic integrals at singular values in quantum field theory [2, 8]. However, that was done more labouriously, without benefit of the novel construction in (23–26).

The discoveries reported here stemmed from my persistent belief that (notwithstanding well-intentioned advice to the contrary) the problem of a polynomial with degree $3h$, for singular values k_N with $N \equiv 3 \pmod{8}$, ought (at bottom) to be no more difficult than the problem with degree h , for $N \equiv 7 \pmod{8}$.

It was thus rather gratifying to discover that $3 \pmod{8}$ is, in fact, far preferable to $7 \pmod{8}$. In particular, I remark that:

1. The polynomial G in (28) generates the Hilbert class field with great (perhaps unprecedented) economy for large $N \equiv 3 \pmod{8}$ and coprime to 3, since it is precisely the trebling of roots of the Weber polynomial that allowed me to combine their reciprocals, three at a time. Thus we may avoid the large- N growth of $r = \exp(\pi\sqrt{N}/24) + o(1)$, using a level-48 class invariant with growth

$$g = \alpha(N) \exp(\pi\sqrt{N}/48) + o(1) \quad (41)$$

where the asymptotic prefactor $\alpha(N) \in [-\sqrt{2}, \sqrt{2}]$ is given by the signature (23) as

$$\alpha(N) = \begin{cases} -\sqrt{1-\beta_-} = \sqrt{2} \cos(11\pi/16) & \text{for } N \equiv 35 \pmod{64} \\ -\sqrt{1-\beta_+} = \sqrt{2} \cos(9\pi/16) & \text{for } N \equiv 11 \pmod{64} \\ -\sqrt{1+\beta_-} = \sqrt{2} \cos(13\pi/16) & \text{for } N \equiv 51 \pmod{64} \\ -\sqrt{1+\beta_+} = \sqrt{2} \cos(15\pi/16) & \text{for } N \equiv 59 \pmod{64} \\ +\sqrt{1-\beta_-} = \sqrt{2} \cos(5\pi/16) & \text{for } N \equiv 3 \pmod{64} \\ +\sqrt{1-\beta_+} = \sqrt{2} \cos(7\pi/16) & \text{for } N \equiv 43 \pmod{64} \\ +\sqrt{1+\beta_-} = \sqrt{2} \cos(3\pi/16) & \text{for } N \equiv 19 \pmod{64} \\ +\sqrt{1+\beta_+} = \sqrt{2} \cos(\pi/16) & \text{for } N \equiv 27 \pmod{64} \end{cases} \quad (42)$$

with

$$\beta_{\pm} = \sqrt{\frac{1}{2} \pm \sqrt{\frac{1}{8}}} \quad (43)$$

obtained from (26) in the limit $r \rightarrow \infty$.

2. I find it notable that a novel solution to a problem relating to elliptic integrals was suggested, almost by accident, by typing merely 3 primes into Neil Sloane's wonderful search engine for integer sequences [28], which shrewdly informed me of a common residue.
3. The challenge of increasing the value N , of a square-free number for which the complete elliptic integral K_N has been successfully reduced to explicit radicals and Γ values, is now seen to be *far* easier for $N \equiv 3 \pmod{8}$ than for $N \equiv 7 \pmod{8}$, since the minimum value of $h(-N)$ accessible using the residue 3 mod 8 is approximately 3 times smaller than that for 7 mod 8, for comparable N .
4. The cause is clear: we know the result for the sum of Kronecker symbols in [14, Cor. 5.3.13]

$$\sum_{k=1}^{\frac{N-1}{2}} \left(\frac{-N}{k} \right) = \begin{cases} 3h(-N) & \text{for } N \equiv 3 \pmod{8} \\ h(-N) & \text{for } N \equiv 7 \pmod{8} \end{cases} \quad (44)$$

and have very little reason to expect the left-hand side of this equation to favour one residue of N over another, on average.

5. Indeed it does not. The smallest known odd class number $h(-N)$ for $N > 2100000$ and $N \equiv 3 \pmod{8}$ is $h(-2317723) = 105$, while the smallest for $N \equiv 7 \pmod{8}$ is $h(-2140807) = 309$. As expected, from the right-hand side of (44), the latter is close to 3 times former. It might have been thought, heretofore, that what we gained on Kronecker's swings, by choosing 3 mod 8, would be lost on Weber's roundabouts so to speak², where we are confronted by a Weber polynomial with degree $3h$ for the residue 3 mod 8.
6. However, I have demonstrated that nothing is lost, thanks to the construction in (23–26) which gives a pair of class invariants, both of whose minimal polynomials have (conjecturally) degree h for all square-free $N > 1099$ with $N \equiv 3 \pmod{8}$ and N coprime to 3. One of these appears to outperform the double eta-quotient method.
7. It is understandable why the residue 3 modulo 8 was discarded [1, Sect. 7.2.2, p. 46] in the early days of elliptic curve primality proving: the factor 3 in the degree $3h$ of the Weber polynomial appeared to be a considerable hindrance. Yet it is, in reality, a great *help* in generating the class field of degree h , with true economy.
8. For $N = 9760387 \equiv 3 \pmod{8}$, mentioned in an update [22, Table 3] on progress [12] with elliptic curve primality proving, the minimal polynomial G of the level-48 class invariant g in (24) has a height whose *logarithm* is less than 37% of the logarithmic height generated by the double eta-quotient used in *Pari-GP*. Moreover, the far simpler polynomial G was generated by (30) in less than 60% of the time taken by `quadhilbert(-9760387)` in *Pari-GP*.
9. After completing this work, I found that the cubic relative extension (18) had been analyzed in [24, 29, 33] in cases with class number $h(-N) \leq 5$.

I conclude by remarking that negative discriminants $D = -N$ with $N \equiv 3 \pmod{8}$ have recently been used to good effect in the construction of elliptic curves of prime order [11] as well as in elliptic curve primality proving [19, 22]. It may be that the class invariants $[f, g]$ constructed in (24) have something to offer researchers in these and other fields. To that end, I append a polynomial, derived from (19,20), that relates g to the j -invariant.

²The colloquial saying seems to be: “What’s lost upon the roundabouts, we pull up on the swings.”

7 Appendix

With $J = j((1 + \sqrt{-N})/2)$ and $[f, g]$ defined in (24) for $N \equiv 3 \pmod{8}$, I obtained

$$\begin{aligned}
& 4722366482869645213696g^{192} + 906694364710971881029632g^{189} \\
& + 83642555144587156024983552g^{186} + 4939066436035567493262082048g^{183} \\
& + 209846732144453295821190856704g^{180} + 6836790472875669456820597948416g^{177} \\
& + 177760660111365660798399713116160g^{174} + 3790405367998157254338394567213056g^{171} \\
& + 67599317184302478754990860798001152g^{168} + 1023330374861490173762756220786049024g^{165} \\
& + 13300167538995234485451503275754913792g^{162} + 149751357319880860617353032541637967872g^{159} \\
& + 1471242473645701356762195242184643444736g^{156} + 12686152623120457776559166922665911910400g^{153} \\
& + 96465713862314370555819332777575421313024g^{150} + 649387270593628934858171069925186898755584g^{147} \\
& + (31230955333453581854030430208J + 3882453146659327990928087554832136180596736)g^{144} \\
& + (3112575311968735739497345449984J + 20668528534099939341664223139973218586066944)g^{141} \\
& + (146491081273850273193327964717056J + 98181174566531282177050821993847942140657664)g^{138} \\
& + (4334567835473120225746709693595648J + 416862949310707523391004696461020551773683712)g^{135} \\
& + (90573700669027853953409791435997184J + 1584081987345225328419300608733679840703545344)g^{132} \\
& + (1423343973438783107899395237834915840J + 5392827180734138390120670122880709527544528896)g^{129} \\
& + (17493275962926368294467182339498704896J + 16459794382816811643862933127629261242032455680)g^{126} \\
& + (172648676792410562129703110693458280448J + 45061910572250059933411888109783903591347519488)g^{123} \\
& + (1394283125785794590584373780949472641024J + 110684289672788641685181184738158837724230975488)g^{120} \\
& + (9342192287286270079567239190370043559936J + 243939817239193661299082038559564687476650934272)g^{117} \\
& + (52479612331578998117553933098199803756544J + 482336992597299364139466938834793244884021018624)g^{114} \\
& + (249139788648436660109159830308175969517568J + 855388454309670556943328874006671088228310712320)g^{111} \\
& + (1005715446292108629597040700247216865935360J + 1359908516549423968069669760282605503992983191552)g^{108} \\
& + (3468496180439370615221376712976872425652224J + 1936722218974592826488979701653464696769575124992)g^{105} \\
& + (10256774471149943627485447340354884299915264J + 2468005608190905568464422101020736836421097095168)g^{102} \\
& + (26077249048140483395956375421712523558125568J + 2809141400052941240710393397868547027567342780416)g^{99} \\
& + (74434605568023196281142352281600J^2 + 57114891944394614356435459851412372728053760J \\
& + 2847596261406655579330927459837021685211463680000)g^{96} + (2477554196157529183058923534417920J^2 \\
& + 107908793049662694542903803183229293591265280J + 2557916576434113812829574035094728838099498958848)g^{93} \\
& + (37777050131731872831172646094766080J^2 + 176007812462339450094643683054165114857979904J \\
& + 2018094067316585479424095293307588682510015397888)g^{90} + (350315392609385120206628736534052864J^2 \\
& + 247919707199861830348868071022250230292676608J + 1375480968524779058279375724416284358713081331712)g^{87} \\
& + (2212954931060628055518534721471512576J^2 + 301530529184884050981024118577114960445308928J \\
& + 782912651925726045755575568707697403306226745344)g^{84} + (10113655478296307547676853277516890112J^2 \\
& + 316467192335142296745902365499603998948196352J + 342002381493088167709431759538867103984517120000)g^{81} \\
& + (34686160560417913758497734880697253888J^2 + 286296268001635388526891108596990972415442944J \\
& + 80670074215058098900212634195910829748908982272)g^{78} + (91454819947811608348373674411331420160J^2 \\
& + 222854932560540399953035451922185320440791040J - 32576013459072580759743422218374296690436866048)g^{75} \\
& + (188538486053819166866726313869734576128J^2 + 148855954137712460111900655737028200724692992J \\
& - 55144112538101344960539779845043749378943090688)g^{72} + (307688231969241589959784881772377931776J^2 \\
& + 84952975352400749448181433286283669083783168J - 39652008878894560091506319036249518347078598656)g^{69} \\
& + (401243764881273752344676821704124661760J^2 + 41126233908050171152515472191400945995743232J \\
& - 18737893972438524931145834580573490329621102592)g^{66} + (421140463268410135952689102182263291904J^2 \\
& + 16667390579331302318343971161533721635454976J - 5174077032622993644412698123126373574057656320)g^{63} \\
& + (357737370032797306669416932583241940992J^2 + 5506258143473539813062973804040786515329024J \\
& + 356706547547601649023766058702724252706013184)g^{60} + (246929031550304841851998761113119358976J^2 \\
& + 1391923871860051857163468765410511483305984J + 1324523691432456084761088145116209617060233216)g^{57} \\
& + (138863115636906600095701410448505044992J^2 + 218444669720290975310036847391841483489280J \\
& + 806529800268765371684542515696435618323103744)g^{54} + (63697798479377155669175763462382419968J^2 \\
& - 5462276197319471266819439416672115490816J + 266980239729130899108909660949569834722525184)g^{51} \\
& + (698176579929963364344659968J^3 + 23826118069257453400721993188748820480J^2
\end{aligned}$$

$$\begin{aligned}
& -13455662359513885691724184271536483467264J + 25376524169352783195973261633263764798177280)g^{48} \\
& + (2550985327389109428468842496J^3 + 7253560775325956917535952133876088832J^2 \\
& - 1613591086910774630703152810299985231872J - 24065084574987736253843103599575646487969792)g^{45} \\
& + (4174917207070705118814928896J^3 + 1790785455303357581601357069218217984J^2 \\
& + 1787431768056365804275779798027674320896J - 14211863708323917478342629778282407593508864)g^{42} \\
& + (4040205466878976552201093120J^3 + 356547255740949811729208872745828352J^2 \\
& + 1125486365607802615981912345130657906688J - 3441206898378612596310745579245155244834816)g^{39} \\
& + (2570697570474836080757047296J^3 + 56806582737949670581168990750507008J^2 \\
& + 226614072500397724462829613101904560128J - 112335117391643625302204517357601891024896)g^{36} \\
& + (1131315371638572737196195840J^3 + 7167453070918708350458449780277248J^2 \\
& - 87239165909372962210788016406434676736J + 192249493128040752962179905607616239239168)g^{33} \\
& + (35274045577859128457691136J^3 + 706517742750046477475912431435776J^2 \\
& - 64776713258997636457464555907753967616J + 66506990142748686364267453679736522276864)g^{30} \\
& + (78521574805087093933473792J^3 + 53633593765131740994404867899392J^2 \\
& - 10038379384210031276177488830957355008J + 7410964829180529718510440126722403729408)g^{27} \\
& + (12416913717118929289347072J^3 + 3135707043050900857899932712960J^2 \\
& + 1593542960922142737017862254701314048J - 659117895483763817020809120277963210752)g^{24} \\
& + (1371359778179842251423744J^3 + 108551055367292136549255217152J^2 \\
& + 405810458730443210149413338518388736J - 482780631328626439347360470569198813184)g^{21} \\
& + (102588738647821241548800J^3 + 64988007965336090461895393280J^2 \\
& - 1063100916132737610564329604644864J - 65330166994701834714296174655572017152)g^{18} \\
& + (4951224026747224719360J^3 - 38854100569579258684962242560J^2 \\
& - 1959825089179216758355828729184256J - 2155988932398684231421595412269629440)g^{15} \\
& + (142903607317254504448J^3 + 7056016192482886441475506176J^2 \\
& - 32318350469538093301391589113856J + 1183943345005433116201363571887570944)g^{12} \\
& + (2182827387064418304J^3 - 415803546176586840262311936J^2 \\
& + 1949335548919313469500521709568J + 185598558328963647368433135255552000)g^9 \\
& + (14241167385034752J^3 + 6745596914666936897372160J^2 \\
& - 90486773832711112570699776000J + 9948227935453805037037289472000000)g^6 \\
& + (25348472307712J^3 - 19845426622060560384000J^2 \\
& + 4189061192520522792960000000J + 181543631801412552228864000000000)g^3 \\
& + J^4 + 2654208000J^3 + 2348273369088000000J^2 + 692533995824480256000000000J = 0.
\end{aligned}$$

The corresponding polynomial relation for f has degree 8 in J and is likewise available in the file `PhiJFG.txt` with checks provided by `PhiJFG.gp` and `PhiJFG.out` from the URL in the first footnote.

Acknowledgements

I am very grateful to David Bailey, Karim Belabas, John Bolton, Jon Borwein, Reinier Bröker, Chris Caldwell, Larry Glasser, Marcel Martin, Neil Sloane and John Zucker for their generous advice and gentle encouragement.

References

- [1] A.O.L. Atkin and F. Morain, “Elliptic curves and primality proving”, *Math. Comp.*, **61** (1993), 29–66.
- [2] David H. Bailey, Jonathan M. Borwein, David Broadhurst and M.L. Glasser, “Elliptic integral evaluation of Bessel moments and applications”, *J. Phys. A: Math. Theor.*, **41** (2008), 205203 (46pp), <http://arxiv.org/abs/0801.0891> .
- [3] D. Bailey, J. Borwein, N. Calkin, R. Girgensohn, R. Luke and V. Moll, *Experimental Mathematics in Action*, AK Peters, 2007.
- [4] Bruce C. Berndt, Heng Huat Chan and Liang–Cheng Zhang, “Ramanujan’s class invariants, Kronecker’s limit formula, and modular equations”, *Trans. Amer. Math. Soc.*, **349** (1997), 2125–2173.
- [5] Bruce C. Berndt, Blair K. Spearman and Kenneth S. Williams, “Commentary on an unpublished lecture by G.N. Watson on solving the quintic”, *The Mathematical Intelligencer*, **24:4** (2002), 15–33, also available from <http://www.math.uiuc.edu/~berndt/articles/watsonlecture.pdf> .
- [6] A. Borel, S. Chowla, C.S. Herz, K. Iwasawa and Jean–Pierre Serre, *Seminar on complex multiplication*, Princeton, N.J., USA 1957–58, Springer Lecture Notes in Mathematics, **21**, 1966.
- [7] Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM: a study in analytic number theory and computational complexity*, CMS Monographs and Advanced Books in Mathematics, John Wiley, Hoboken, NJ, 1987.
- [8] David Broadhurst, “Elliptic integral evaluation of a Bessel moment by contour integration of a lattice Green function”, preprint, 6 February 2008, <http://arxiv.org/abs/0801.4813> .
- [9] David Broadhurst, “Algebraic integers at the singular value k_{34483} ”, posting to the NMBRTHRY list, 30 March 2008, <http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0804&L=nmbnthry&P=R342> .
- [10] David Broadhurst, “Singular values of elliptic integrals in quantum field theory”, talk at the workshop *Loops and legs in quantum field theory*, Sonderhausen, 25 April 2008, <http://physics.open.ac.uk/~dbroadhu/singval.pdf> .
- [11] Reinier Bröker, “Constructing elliptic curves of prime order”, Thesis, Universiteit Leiden, 2006, <http://www.math.leidenuniv.nl/scripties/Broker.pdf> .
- [12] Chris Caldwell, “Elliptic curve primality proof”, record primes of this type, tabulated at <http://primes.utm.edu/top20/page.php?id=27> .
- [13] S. Chowla and A. Selberg, “On Epstein’s zeta–function (I)”, *Proc. Nat. Acad. Sci. USA*, **35** (1949), 371–374.
- [14] Henri Cohen, *A course in computational algebraic number theory*, Springer, 1996.
- [15] A. Enge and R. Schertz, “Constructing elliptic curves over finite fields using double eta-quotients”, *J. Théor. Nombres Bordeaux*, **16** (2004), 555–568.
- [16] Farshid Hajir and Fernando Rodriguez Villegas, “Explicit elliptic units, I”, *Duke Math. J.*, **90** (1997), 495–521.

- [17] James G. Huard, Pierre Kaplan and Kenneth S. Williams, “The Chowla–Selberg formula for genera”, *Acta Arith.*, **73** (1995), 271–301.
- [18] James G. Huard and Kenneth S. Williams, reply to a letter to the editor, *Notices of the American Mathematical Society*, **45:8** (1998), 951.
- [19] Marcel Martin, “Primo – primality proving”, single-processor ECPP software available from <http://www.ellipsa.net/public/primo/primo.html> .
- [20] F. Morain, “Courbes elliptiques et tests de primalité”, Thesis, Université de Lyon I, 1990, <ftp://ftp.inria.fr/INRIA/publication/Theses/TU-0144/> .
- [21] F. Morain, “Modular curves and class invariants”, talk at the L.M.S. Durham Symposium on Computational Number Theory, July 2000, with slides in the file [durham2000.ps.gz](http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/durham2000.ps.gz) available from <http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/> .
- [22] F. Morain, “Implementing the asymptotically fast version of the elliptic curve primality proving algorithm”, *Math. Comp.*, **76** (2007) 493–505.
- [23] Jan Nekovář, letter to the editor, *Notices of the American Mathematical Society*, **46:2** (1999), 190.
- [24] R. Russell, “On modular equations”, *Proc. London Math. Soc.*, **21** (1890), 351–395.
- [25] Reinhard Schertz, “Construction of ray class fields by elliptic units”, *J. Théor. Nombres Bordeaux*, **9** (1997), 383–394.
- [26] Reinhard Schertz, “Weber’s class invariants revisited”, *J. Théor. Nombres Bordeaux*, **14** (2002), 325–343.
- [27] A. Selberg and S. Chowla, “On Epstein’s zeta–function”, *J. Reine Angew. Math.*, **227** (1967), 86–110.
- [28] N.J.A. Sloane, *The on-line encyclopedia of integer sequences*, available at <http://www.research.att.com/~njas/sequences/index.html> .
- [29] G. N. Watson, “Some singular moduli (I)”, *Quart. J. Math.*, **3** (1932), 81–98; “Some singular moduli (II)”, *Quart. J. Math.*, **3** (1932), 189–212; “Singular moduli (3)”, *Proc. London Math. Soc.*, **40** (1936), 83–142; “Singular moduli (4)”, *Acta Arith.*, **1** (1936), 284–323; “Singular moduli (5)”, *Proc. London Math. Soc.*, **42** (1937), 377–397; “Singular moduli (6)”, *Proc. London Math. Soc.*, **42** (1937), 398–409.
- [30] Heinrich Weber, *Lehrbuch der Algebra*, Vol. 3, 2nd edition, Braunschweig, 1908, reprinted by AMS Chelsea, 1961.
- [31] J.M. Whittaker, “George Neville Watson. 1886–1965”, *Memoirs of Fellows of the Royal Society*, **12** (1966), 521–530.
- [32] G.P. Young, “Solvable quintic equations with commensurable coefficients”, *Amer. J. Math.*, **10** (1888), 99–130.
- [33] Noriko Yui and Don Zagier, “On the singular values of Weber modular functions”, *Math. Comp.*, **66** (1997), 1645–1662.
- [34] I.J. Zucker, “The evaluation in terms of Γ –functions of the periods of elliptic curves admitting complex multiplication”, *Math. Proc. Cambridge Philos. Soc.*, **82** (1977), 111–118.